IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

SPENCER BUENO, on behalf of himself and all others similarly situated,

Plaintiff,

v.

ARHAUS, LLC,

Defendant.

Case No. 5:22-cv-01624

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

INTRODUCTION

1. Plaintiff, Spencer Bueno ("Mr. Bueno" or "Plaintiff"), through his attorneys, brings this Class Action Complaint against the Defendant, Arhaus, LLC ("Arhaus" or "Defendant"), alleging as follows.

2. Arhaus, a publicly traded company with over 1,000 employees, lost control over its employees' highly sensitive personally identifying information ("PII") to hackers in a cybersecurity breach ("Data Breach"). Despite recognizing the risk that security breaches pose to Arhaus's employees and its responsibility to quickly warn them about data breaches, Arhaus failed to implement reasonable security measures to safeguard employee PII, which was open to hackers for *two full months*. In that time, Arhaus employees were unable to protect their identities and proactively mitigate the Data Breach's impact on them. Mr. Bueno is a former Arhaus employee and Data Breach victim. In the months that Arhaus waited to disclose the Data Breach, cybercriminals stole Mr. Bueno's PII and posted it on the dark web. Mr. Bueno brings this Class Action on behalf of himself and all individuals harmed by Arhaus's conduct.

3. On June 24, 2021, Arhaus discovered that hackers had breached its systems and accessed employee PII. Although Arhaus says that its investigation of the Data Breach "did not find any evidence indicating that any emails or attachments were actually accessed or exported from the accounts," in reality it lost control over employee PII to cybercriminals, allowing criminals access to employee "name, driver's license number, Social Security number, and/or financial account information."

4. Plaintiff Spencer Bueno is a victim of the data breach. He was an Arhaus employee in 2021 and 2022, during which time Arhaus collected his PII as a condition of employment. As a result of Arhaus's failure to take reasonable precautions, wrongdoers accessed Bueno's PII, thereby subjecting him to a severe invasion of privacy.

5. Bueno, on behalf of himself and all others similarly situated, seeks damages and equitable relief for Arhaus's negligence, breach of confidence, breach of contract, and (alternatively) unjust enrichment.

PARTIES

6. Plaintiff Spencer Bueno is currently a resident of San Diego, California. At the time of his employment with Arhaus, Plaintiff was a resident of Pompano Beach, Florida.

7. Defendant Arhaus, LLC is a Delaware corporation with its principal place of business in Boston Heights, Ohio. Its headquarters is located at 51 E. Hines Hill Road, Boston Heights, Ohio 44236.

JURISDICTION AND VENUE

8. Arhaus is subject to this Court's personal jurisdiction because its principal place of business is (and at all relevant times was) located in Boston Heights, Ohio.

9. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332(d)(2) because at least one member[1] of the proposed Class is a citizen of a state different from that of Arhaus; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 class members, and none of the exceptions under the subsection apply to this action.

10. Venue is proper in the Northern District of Ohio, Eastern Division because a substantial part of the events and omissions giving rise to this claim occurred in Summit County. *See* 28 U.S.C. § 1391(b)(2); S.D. OHIO CIV. R. 82.1(b)–(d). Specifically, Arhaus's headquarters is located in Summit County where, on information and belief, it made the relevant decisions giving rise to the data breach.

FACTUAL ALLEGATIONS

A. Arhaus.

11. Arhaus is a high-end home furnishings manufacturer. In 2021, Arhaus was first listed on the NASDAQ exchange, with an Initial Public Offering valued at $1.75 billion.[2]

12. Arhaus's internal policies recognize Arhaus's responsibility for maintaining and securing sensitive data, including employee PII.

13. Arhaus represents to the public that "We have implemented commercially reasonable and appropriate physical, technical, and administrative

[1] Arhaus submitted data breach notifications indicating that at least one citizen from Massachusetts and two from Montana were affected by the breach. *See* Massachusetts Office of Consumer Affairs and Business Regulation, *Data Breach Notification Letters July 2022* (2022), https://www.mass.gov/lists/data-breach-notification-letters-july-2022; Montana Department of Justice, *Reported Data Breach Incidents* (accessed September 9, 2022), https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-423.pdf. On information and belief, the Class includes residents of other states as well.

[2] https://www.forbes.com/sites/pamdanziger/2021/11/05/specialty-home-furnishings-retailer-arhaus-underwhelms-in-its-nasdaq-open/?sh=626bb7807f6e (accessed September 11, 2022).

safeguards to help prevent unauthorized access to, use of, and disclosure of, [ ] personal information."[3]

14. But, on information and belief, Arhaus fails to strictly adhere to these policies, leaving vulnerabilities in its systems for cybercriminals to exploit.

B. Arhaus Fails to Safeguard Employee PII

15. Plaintiff Bueno and the proposed Class are current and former Arhaus employees.

16. As a condition of employment with Arhaus, Arhaus requires its employees to disclose their PII, including their names, addresses, dates of birth, Social Security or individual tax identification numbers, driver's license or other government issued identification card numbers, as well as health-related information, health insurance policy or member numbers, financial account information, and fingerprints.

17. In collecting and maintaining the PII, Arhaus agreed it would safeguard the data according to its internal policies and state and federal law

18. Arhaus collects and maintains employee PII in its computer systems.

19. Despite its representations and undertaken responsibilities, Arhaus allowed cybercriminals to access PII in its systems during a period from March 25, 2022 to May 24, 2022 (the Data Breach).

20. Arhaus does not tell a consistent story about the Data Breach. In its representative letter to the Montana Attorney General (and to Plaintiff Bueno), Arhaus represents that "[a]lthough our investigation did not find any evidence indicating that any emails or attachments were actually accessed or exported from

[3] https://www.arhaus.com/pages/privacy-policy#info-security (accessed September 11, 2022).

the accounts, we cannot definitively rule out that possibility."[4] By contrast, the letter to the Massachusetts Attorney General states that the incident "involved your name and Social Security number."[5]

21. Either way, Arhaus conducted an "investigation" on June 24, 2022.

22. But it was not until July 22, 2022, that Arhaus informed affected employees and former employees such as Plaintiff Bueno that their information had been compromised. At true and correct copy of the Breach Notice is attached as Exhibit A to the Complaint.

23. Until that time, Plaintiff Bueno and the proposed Class had no idea their PII had been compromised in a data breach and thus could not proactively mitigate the Data Breach's impact on them.

24. The Breach Notice Plaintiff Bueno received attempts to minimize the potential impact of the Data Breach, stating that it was informing affected individuals "out of an abundance of caution," the other versions of the release paint a different, and likely more accurate, picture.

25. The Breach Notice acknowledged the ongoing threat the Data Breach posed to its current and former employees, offering them credit monitoring services. But the "free" services continued for only one to two years.

26. On information and belief, Arhaus failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. Arhaus's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Arhaus cannot or will

---

[4] https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-423.pdf (accessed September 11, 2022).

[5] https://www.mass.gov/doc/assigned-data-beach-number-27928-arhaus-inc/download (accessed September 11, 2022).

not even determine the full scope of the Data Breach, as it has evidently been unable to determine exactly what information was stolen and when.

C. Plaintiff's Experience.

27. As part of its business model, Arhaus maintains a series of retail showrooms throughout the country. Plaintiff Bueno was employed as a salesperson in the Boca Raton, FL location from November 2021 to February 21, 2022.

28. Consistent with Arhaus's mandatory policies, Plaintiff Bueno provided his PII to Arhaus as a condition of employment. Plaintiff Bueno did so based on a trust that Arhaus would use reasonable measures to protect it according to Arhaus's internal policies and state and federal law.

29. Following the Data Breach from March to May 2022, Arhaus did not inform Plaintiff Bueno about the breach, and he did not know that his information had been compromised in the Data Breach.

30. Because Arhaus did not immediately disclose the breach, Plaintiff Bueno was unable to take precautionary measures earlier, meaning his PII was unprotected.

31. Instead, Plaintiff Bueno received an alert via Experian that his Social Security Number had been posted to the "dark web." On information and belief, the "dark web" is an internet portal where compromised identities can be traded or sold by cybercriminals

32. Plaintiff Bueno has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Bueno fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. He has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes

far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

33. Further, Plaintiff Bueno is unsure what has happened to his PII because Arhaus has not disclosed the true nature of the Data Breach or what measures it is taking to safeguard his PII in the future.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft.

34. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

35. As a result of Arhaus's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;
b. The diminution in value of their PII;
c. The compromise and continuing publication of their PII;
d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
f. Delay in receipt of tax refund monies;
g. Unauthorized use of stolen PII; and
h. The continued risk to their PII, which remains in the possession of Arhaus and is subject to further breaches so long as Arhaus

fails to undertake the appropriate measures to protect the PII in their possession.

36. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00, depending on the type of information obtained.

37. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course. That is what happened to Plaintiff Bueno in this case.

38. It can take victims years to spot identity or PII theft, giving criminals plenty of time to mine that information for cash.

39. One such example of criminals using PII for profit is the development of "Fullz" packages.

40. Cyber-criminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

41. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and

members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

CLASS ACTION ALLEGATIONS

42. Pursuant to FED. R. CIV. P. 23(b)(3), Plaintiff seeks certification of a class defined as follows:

> All individuals residing in the United States whose PII was compromised in the Data Breach of Arhaus occurring between March 25, 2022 and May 24, 2022.

43. Excluded from the Class are: (a) Arhaus and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

44. *Ascertainability*. The Class can be readily identified through Arhaus's records, which is demonstrated by the fact that Arhaus has already identified the class members and notified them of the breach. *Notice of Data Breach*, Exhibit 1.

45. *Numerosity*. Arhaus has well over one thousand employees, and thus the class is of a similar size—far too many to join in a single action.

46. *Typicality*. Plaintiff's claims are typical of the Class he seeks to represent. Like all class members, Plaintiff's personal information was exposed in the data breach as a result of Arhaus's' failure to implement reasonable data security measures. Thus, Plaintiff's claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

47. *Adequacy of Class Representative.* Plaintiff will fairly and adequately protect the interests of the Class. He is aware of his fiduciary duties to absent class

members and is determined to faithfully discharge his responsibility. Plaintiff's interests are aligned with (and not antagonistic to) the interests of the Class.

48. *Adequacy of Counsel.* In addition, Plaintiff has retained competent counsel with considerable experience in class action and other complex litigation, including data breach cases. Plaintiff's counsel have done substantial work in identifying and investigating potential claims in this action, have considerable knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Class.

49. *Commonality and Predominance.* This case presents numerous questions of law and fact with answers common to the Class that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Arhaus had a duty to use reasonable care to safeguard Plaintiff and the Class's PII;

b. Whether Arhaus failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach

c. Whether Arhaus breached the duty to use reasonable care to safeguard the Class's PII;

d. Whether Arhaus breached its contractual promises to safeguard Plaintiff and the Class's PII;

e. Whether Arhaus knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

f. Whether Arhaus failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

g. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Arhaus's computer systems to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

h. Whether the data breach was caused by Arhaus's inadequate cybersecurity measures, policies, procedures, and protocols;

i. Whether Arhaus took reasonable measures to determine the extent of the data breach after it was discovered;

j. Whether Arhaus's method of informing Plaintiff and other the Class of the data breach was unreasonable;

k. Whether Arhaus is liable for negligence, gross negligence, or recklessness;

l. Whether Arhaus's conduct, practices, statements, and representations about the data breach of the PII violated applicable state laws;

m. Whether Plaintiff and the Class were injured as a proximate cause or result of the data breach;

n. Whether Plaintiff and the Class were damaged as a proximate cause or result of Arhaus's breach of its contract with Plaintiff and the Class;

o. What the proper measure of damages is; and

p. Whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

50. *Superiority and Manageability*. A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

CAUSES OF ACTION

Count 1: Negligence

51. Plaintiff incorporates by reference all of the above allegations.

52. Plaintiff and the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

53. Defendant owed a duty of care to Plaintiff and the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the data breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and the Class's PII failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

54. Defendant owed to Plaintiff and the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and the Class the scope, nature, and occurrence of the data breach. This duty is necessary in order for Plaintiff and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the data breach.

55. Defendant owed these duties to Plaintiff and the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and the Class's personal and financial information and PII as a condition of employment, and Defendant retained that information.

56. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds significant quantities of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

57. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

58. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and the Class which actually and proximately caused the data breach and Plaintiff and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and the Class's injuries-in-fact.

59. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and the Class's actual, tangible, injury-in-fact and damages, including, without limitation, theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

Count 2: Negligence Per Se

60. Plaintiff incorporates by reference all of the above allegations.

61. Defendant is a "business entity" that maintains, stores, or manages computerized data that includes "personal information" as defined by Ohio R.C. § 1349.19(A).

62. Plaintiff and the Class's PII includes "personal information" as defined by Ohio R.C. § 1349.19(A).

63. Defendant was aware of a breach of its computer system that it believed or reasonably should have believed had caused or would cause loss or injury.

64. Defendant had an obligation to disclose the data breach to Plaintiff and the Class in a timely fashion as mandated by Ohio R.C. §§ 1349.19(B)(1)-(2).

65. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII and to notify Plaintiff and the Class if the security of their PII was compromised.

66. Defendant breached its duties to Plaintiff and the Class under Ohio R.C. §§ 1349.19(B)(1)-(2) by failing to provide fair, reasonable, adequate, or timely notice of the data breach to Plaintiff and the Class.

67. Defendant's failure to disclose the data breach in a timely manner as required by Ohio R.C. § 1349.19(B) constitutes negligence per se.

68. As a direct and proximate cause of Defendant's negligence in failing to timely notify them of the data breach, in violation of Ohio R.C. § 1349.19(B), Plaintiff and the Class sustained actual losses and damages as described in this complaint.

69. In addition, pursuant to the FTC Act, 15 U.S.C. § 45, Arhaus had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

70. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

71. Arhaus violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Arhaus's conduct was particularly unreasonable given the nature and amount of PII that Arhaus had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

72. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

73. Arhaus had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

74. Arhaus breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

75. Arhaus's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

76. As a direct and proximate result, Plaintiff suffered actual losses and damages, including, without limitation, theft of his PII by criminals, improper disclosure of his PII, lost value of his PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Arhaus's negligence

Count 3: Breach of Implied Contract

77. Plaintiff incorporates by reference all of the above allegations.

78. Defendant offered employment to Plaintiff and members of the Class in exchange for their PII.

79. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects from employees to unauthorized persons. Defendant also promised to safeguard employee PII.

80. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

81. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

82. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

83. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

84. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

85. Plaintiff and the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

86. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

87. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

88. Defendant failed to advise Plaintiff and the Class of the data breach promptly and sufficiently.

89. Defendant also failed to provide adequate data security, even though it knew that Plaintiff and the Class understood Defendant would safeguard their PHI and would not have provided their PII to Defendant absent such understanding.

90. In these and other ways, Defendant violated its duty of good faith and fair dealing.

91. Plaintiff and the Class have sustained damages as a result of Defendant's breaches of the agreement.

Count 4: Unjust Enrichment

(In the Alternative to Count 3)

92. Plaintiff incorporates by reference paragraphs 1–84 of this complaint.

93. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

94. Plaintiff and the Class conferred a monetary benefit upon Defendant in the form of services through employment.

95. Plaintiff and members of the Class worked for Defendant for a specified rate of remuneration that contemplated Defendant would take adequate safeguards to protect their PII.

96. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to facilitate their employment.

97. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

98. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class because Defendant failed to implement (or adequately implement) the data privacy and

security practices and procedures for itself that Plaintiff and the Class paid for and were otherwise mandated by federal, state, and local laws and industry standards.

99. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

100. Plaintiff, individually and on behalf of all others similarly situated, hereby demands:

a. Certification of the proposed Class;

b. Appointment of the undersigned counsel as class counsel;

c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law;

d. Restitution or disgorgement of all ill-gotten gains; and

e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

101. Plaintiff demands a jury trial on all applicable claims.

Respectfully submitted,

By: /s/ *Matthew R. Wilson*

MEYER WILSON CO., LPA
Matthew R. Wilson (72925)
Trial Attorney
Email: mwilson@meyerwilson.com
Michael J. Boyle, Jr. (91162)
Email: mboyle@meyerwilson.com
Jared W. Connors (101451)
Email: jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice* to be filed)
sam@turkestrauss.com
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

Counsel for Plaintiff and the Proposed Class